(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/91397 A2

(51) International Patent Classification⁷: H04L 29/00

(21) International Application Number: PCT/CA01/00727

(22) International Filing Date: 22 May 2001 (22.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/575,544 22 May 2000 (22.05.2000) US

(71) Applicant: LADR IT CORPORATION [CA/CA]; 6 Sawgrass Circle, Ashton, Ontario K0A 1B0 (CA).

(72) Inventor: SHAWCROSS, Charles, Byron, Alexander; 6 Sawgrass Circle, Ashton, Ontario K0A 1B0 (CA).

(74) Agent: CASSAN, Lynn, S.; Ridout & Maybee, 150 Metcalfe Street, 19th Floor, Ottawa, Ontario K2P 1P1 (CA).

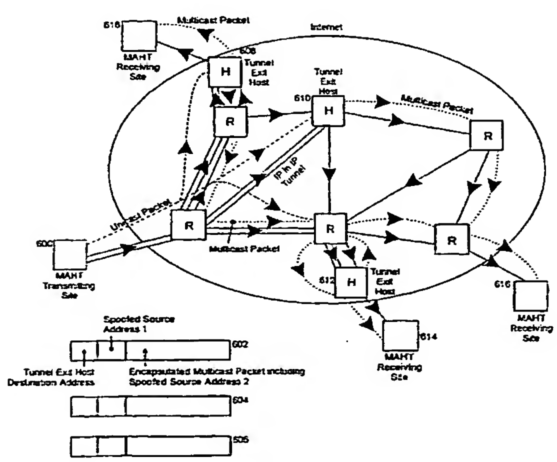
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR ANTI DENIAL OF SERVICE AND ANTI TRAFFIC ANALYSIS CAPABILITIES FOR IP BASED VIRTUAL PRIVATE NETWORKS AND DATA DISTRIBUTION THROUGH USE OF AN IP MULTICAST ADDRESS HOPPING TECHNIQUE



(57) Abstract: A method and system for Internet Protocol network communications and uses thereof for protecting Internet sites against denial of service and traffic analysis attacks on insecure public networks such as the Internet are provided. The method provides for communicating multicast packets between end stations, in a multicast IP network, on a chosen multicast IP address from a plurality of multicast IP addresses for multicast communication using a multicast address hopping technique. The technique selectively varies the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the end stations but not to unauthorized endstations. The packets are then communicated on the chosen multicast IP address. Indicia normally capable of identifying the source of the packets may be selectively varied to conceal the source of the packets. Further, the packets may be communicated to an end station having subscribed to a set of multicast IP addresses comprising at least one multicast IP address from the plurality of multicast IP addresses for multicast communication and including the chosen multicast IP address for transmitting the packets. The set of multicast IP addresses may also be selectively varied according to a secret predetermined scheme known to the end stations, particularly by randomly adding to and dropping from the set of multicast IP addresses. Multiple sets of communicating groups all utilizing the same address space can coexist such that their respective traffic is intermingled on the various addresses, making traffic analysis very difficult. In another embodiment, a data coding scheme such as code division multiplexing may be employed on the individual multicast packets data fields to allow data for individual destinations to be mixed together in one packet that is multicast to a plurality of receivers. Each receiver then decodes its applicable data by passing the received multicast data field through the appropriate decoding scheme such as a code division de-multiplexing process. In further aspects of the invention, various uses of the invention for Virtual Private Networks and other secure communication systems are also provided.

WO 01/91397 A2

TITLE OF THE INVENTION

METHOD AND SYSTEM FOR ANTI DENIAL OF SERVICE AND ANTI TRAFFIC ANALYSIS CAPABILITIES FOR IP BASED VIRTUAL PRIVATE NETWORKS AND DATA DISTRIBUTION THROUGH USE OF AN IP MULTICAST ADDRESS HOPPING TECHNIQUE

FIELD OF THE INVENTION

The present invention generally relates to a method and system for Internet Protocol network communications and uses thereof for providing enhanced virtual private network capabilities on insecure public networks such as the Internet.

BACKGROUND OF THE INVENTION

An ever-increasing trend is the use of the Internet Protocol (IP) based Internet as a communications network for business to consumer (B2C), business to business (B2B), and consumer to consumer (C2C) interaction and transactions. There is a constantly evolving gamut of threats encountered with respect to IP networks, particularly the Internet. Although a network is just the communication channel through which information is accessed or flows, the interconnection of systems worldwide through networks, especially the Internet, has become so widespread that it has become a key component of modern military, industrial, government, and private systems. The growing dependence of the various systems on a properly functioning network increases their operational vulnerability through disruption of the network. The gamut of threats to IP network based systems includes techniques to steal information, corrupt or alter information, destroy information, deny use of services or information, gather indicators of future action, and affect the public's view of various issues, including social, political, and even confidence in a country's government. The Internet, in particular, is an insecure public network and presents various weaknesses that can

be exploited by criminals or other elements to disrupt or monitor the normal communications between parties on the Internet. Some of these weaknesses include vulnerabilities to various types of Denial of Service (DoS) attacks. Recently, such attacks have successfully disrupted commercial services offered by prominent vendors.

Other vulnerabilities in using a public network for private communications include traffic analysis. Traffic analysis can be defined as the analysis of messages, typically encrypted messages, to determine: where they come from, where they go to, how long they are, when they are sent, how frequent or infrequent they are, whether they coincide with outside events like meetings, and more. There is increasing pressure for industries to gain competitive intelligence (CI) about competitors. This could involve traffic analysis of communications between their competitor various sites or to suppliers or customers. As well, national, military, or criminal entities may use traffic analysis to gain insight into intentions or actual operations of potential or real opponents. Encryption technology is well known and available to provide confidentiality, authentication, and integrity of data transmitted over the Internet. Confidentiality is defined as ensuring only the authorized parties can read the communications. Authentication is defined as ensuring that the communication was actually originated by the party it was purportedly sent by. Integrity is defined as ensuring that the data has not been changed by anyone during the communication process.

Encryption technology forms the basis for Virtual Private Technology (VPN) currently in use on the Internet. A Virtual Private Network is defined as a secure, private network running over a public network such as the Internet. It is created by using software, hardware, or a combination of the two to create a secure link between computers over a public insecure network. This is done through encryption, packet tunneling, and firewalls. Since users can eliminate leased line costs by using the Internet as a Wide Area Network (WAN), a VPN is a cost-effective solution to secure wide area network connectivity. A major disadvantage of such a system under Internet Protocol (IP) is that the packets travel between the two or more sites with identifiable source and destination

addresses. Knowledge of the source and destination addresses allows an attacker to perform certain types of Denial of Service attacks against these sites. Note also that an eavesdropper can observe the volume and timing of the packets. This allows an attacker to perform traffic analysis on this information flow. Thus users of VPN technology are desirous of having a method to prevent traffic analysis against their communications and also to prevent or alleviate the effects of a denial of service attack against their communications.

Denial of Service (DoS) can be defined as action(s) which prevent any part of an automated information system (AIS) from functioning in accordance with its intended purpose or intentional degradation or blocking of computer or network resources. The Computer Emergency Response Team (CERT) at Carnegie Mellon University divides Denial of Service into three modes of attack with sub categories. CERT notes that a Denial of Service may only be a component of a larger attack. The three modes are classified under consumption of scarce resources, destruction or alteration of configuration information, and consumption of other resources. This invention particularly relates to the category of Consumption of Scarce Resources, specifically the sub categories of Bandwidth Consumption, Network Connectivity, and Consumption of Other Resources.

Denial of Service (DoS) attacks are often done through the use of scripts also called tools. A few examples of such tools are Capi, Back Orifice 2000 (BO2K), Domain Name System Attack, and Internet Control Message Protocol (ICMP) ECHO which is based on the ping-flooding concept. These tools are freely available for download from the Internet.

Distributed Denial of Service (DDoS) is an enhanced version of a Denial of Service attack where the DoS tools are distributed to multiple hosts, which can then be coordinated to anonymously perform an attack on the target host simultaneously, typically after some time delay. Some of the currently known Distributed Denial of Service Tools are: Trinoo, Tribe Flood Network (TFN) and Tribe Flood Net 2K, and Stacheldraht (meaning “barbed wire” in German).

Users of the Internet as a communications medium wish to have immunity from Denial of Service attacks that prevent them from using the Internet as they desire. Disruption of this service can be very costly as certain attacks in early February 2000 against major commercial Internet sites demonstrated. Some estimates range as high as $1.2 Billion loss for the several days of attacks.

Users of VPN technology on the Internet still must have identifiable IP addresses used to route the VPN encrypted packets through the network between the VPN nodes. However attackers can use these addresses to direct Denial of Service or traffic analysis attacks against these nodes.

UNICAST IP PACKET ROUTING AND DELIVERY

Traditional Internet protocol (IP) networks rely mostly on the use of unicast protocol (also known as point to point) packet routing and delivery for communications between end stations (for example, a user and a host site). For unicast, a packet is generated and passed into the network by a first end station having the destination address of the second end station as a parameter. This packet is then routed through the network until it is delivered to the end station computer (or is discarded within the network if it times out or a route to the specified address is not found). The destination end station may or may not have been expecting this packet. For example, a ping packet or connection request packet is typically not expected by its recipient. On the other hand, once a connection-oriented communication like TCP/IP (Transmission Control Protocol) has been initiated between the two stations, then each station is in effect expecting packets from the other station and actively accounts for and sends acknowledgements for these packets.

Unicast Packet Routing and Denial of Service Attacks

The important thing to note is that the unicast delivery of packets is based on a "push" system. Packets can be generated and inserted into the

network for delivery to an end station. The end station has little or no control to stop or regulate the flow of certain types of these packets, even if they are causing problems i.e. during an active Denial of Service attack. This "push" protocol forms the weakness that is exploited in many Denial of Service and Distributed Denial of Service attacks occurring on the Internet.

A Denial of Service attack can take the form of a storm of packets addressed to the victim host. This storm of packets can completely clog the communications links into the victim system thus effectively denying service to any legitimate users. The attack can also take the form of using up resources on the target computer such as maximum number of TCP connections. Such an attack can consist of creating multiple TCP connections and then leaving them hanging until they time out. This can use up all the available connection slots thereby denying legitimate users any connections.

Multicast Technology

In contrast to unicast protocol, multicast protocol within an IP network uses a "pull" type system. The destination end station must actively request the reception of these multicast packets by "subscribing" to the router network with special subscription request packets (Internet Group Management Protocol or IGMP) for each multicast address of interest. Once a subscription message is received by a given router from an attached end station the router will autonomously communicate within the network of routing devices to receive the multicast packets with the applicable address. There can be multiple recipients of this traffic flow. If a subscription for a particular address is not renewed periodically by the attached host (typically, in the order of 10's of seconds) then the subscription for that particular address will time out and the router network will no longer route packets for delivery to that particular host. Alternately a host can "de-subscribe" from a given multicast address with a special de-subscribe message to the router which has an immediate impact on the delivery of multicast packets. The important difference between multicast and unicast packet delivery is that

under multicast, the end computer station has control over the addresses from which it will accept data.

Under the current version of the Internet Protocol (IP Version 4 or IPv4), the addresses assigned for multicast are known as Class D addresses and range from the 224.0.0.0 to 239.255.255.255. The Internet Assigned Numbers Authority (IANA) maintains a list of registered users and assigns new numbers for new uses. The range from 224.0.0.0 to 224.0.0.25 is reserved for permanent assignment for various applications, including use by routing protocols. The set from 239.0.0.0 to 239.255.255.255 is reserved for various administratively scoped applications; much the same way as the 192.168.0.0 address range is assigned for administratively scoped unicast purposes. Under IPv6, the emerging new IP version, it is anticipated that there will be 112 bits of information to designate a multicast group. This is a much expanded address space over the current IPv4 allocation that only has 28 bits for address space.

MULTICAST ROUTING PROTOCOLS

Routers in a network or internetwork use multicast routing protocols to efficiently route multicast packets through the network or internetwork much the same as they use unicast (point-to-point) routing protocols to efficiently route unicast packets through the network. The multicast protocols are used to deliver multicast packets from the multicast source to multiple destinations that consist of the members of the multicast group.

Unicast routing protocols use one of two basic techniques, either distance vector (e.g. Routing Information Protocol - RIP), or link state (e.g. Open Shortest Path First - OSPF). Multicast routing protocols can be divided into three categories, distance vector (derived from unicast protocols like RIP), link state (derived from protocols like OSPF), and the newer shared-tree protocols. The multicast protocols in use include: the Distance Vector Multicast Routing Protocol (DVMRP) and Protocol Independent –Dense Mode (PIM-DM) based on distance vector, Multicast Open Shortest Path First (MOSPF) based on link state, and

Protocol Independent – Sparse Mode (PIM-SM) and Core-Base Tree (CBT) based on shared trees. Each of these protocols has their strengths and weaknesses and is employed on various parts of the Internet.

Normally, in any Autonomous System (or domain) within the Internet, there is only one multicast protocol used. An Autonomous System is defined as a network administered by one entity and operating under one unicast routing protocol. A protocol used only within an Autonomous System is referred to as an interior gateway protocol (IGP). The administrative authority for a given Autonomous System specifies which unicast and multicast protocol is to be used within the Autonomous System. The decision is based on a number of factors including the type of routing equipment used in the Autonomous System, personnel experience with the various protocols, expected number of users and groups, and dispersion of users. There are protocols in place for routing unicast between autonomous systems, known as exterior gateway protocols (EGP). Autonomous Systems within the Internet are linked together by routers that use these unicast EGP that enforce routing policies. One weakness of multicast is the lack of an EGP for routing multicast between Autonomous Systems. There is work underway to define interdomain routing protocols, notably the Border Gateway Multicast Protocol (BGMP).

TUNNELING

An IP packet tunneling technique can be used to, among other things, tunnel multicast packets from one area of the Internet to another area of the Internet through an area that does not support multicast. In this technique, the multicast packets are received by a router or host on one end of a tunnel, encapsulated in a unicast IP packet and sent by normal IP unicast to the router or host at the other end of the tunnel where the packets are de-encapsulated and sent back out into the network as multicast packets. This technique is effective but requires a significant amount of administrative overhead. There are various

existing and implemented protocols for IP tunneling in use on the Internet including "IP in IP".

SCOPING

Scoping of multicast packets refers to methods of limiting the range to which a multicast packet can travel in a network. There are presently two main methods used for scoping multicast packets, administrative and Time To Live (TTL) scoping. Administrative scoping involves using the multicast addresses on packets in the address space from 239.0.0.0 to 239.255.255.255. Multicast packets in this range do not cross administrative boundaries. Since multicast addresses are assigned locally within the Autonomous System they need not be unique between areas thus allowing for reuse of address space. TTL scoping refers to placing a low value in the TTL field of a packet when it is initially created. Every IP packet has a data field of one byte that defines a time to live for the packet. Every time the packet crosses a router or similar device or is held in a queue for 30 seconds, the TTL field is decremented. If the TTL reaches zero before the packet reaches its ultimate destination the packet is discarded wherever it is when the TTL reaches zero. Placing a low initial value within the TTL of the packet limits the range to which it can travel.

MULTICAST ADDRESS ALLOCATION

Currently there are very few permanently allocated multicast addresses. Multicast applications are quite free to choose nearly any multicast address for their use. There is a danger of address collision with other applications, so applications must be designed to detect and handle erroneous packets from other applications using the same multicast address. There are methods currently being researched to prevent this problem by providing dynamic multicast address allocation. The current research has defined a three level allocation hierarchy. Within an Allocation Domain, the lower level multicast

applications running on hosts use a Multicast Dynamic Host Control Protocol (MDHCP) (based on the Dynamic Host Control Protocol) to request multicast addresses from the next level Multicast Address Allocation Servers (MAAS). An Allocation Domain normally coincides with the boundaries of the Autonomous System in which it is located. The MAAS's claim multicast addresses allocated through the use of the multicast Address Allocation Protocol (AAP). Certain nodes within the Autonomous System, usually routers, use the Multicast Address Set Claim (MASC) protocol to claim multicast address sets which they allocate to the MAAS's through the AAP. This architecture is experimental and no devices are known that currently support this architecture.

ROUTER INTERFACES

Routers are complex devices designed to efficiently receive and transmit data packets across multiple physical communication channels. These channels can include Ethernet, token ring, serial lines, ATM links, or Frame relay, all with varying characteristics and set up requirements. These channels are normally physically connected to the routers on what are called interfaces. The routers run various protocols that determine how they will receive, process, and transmit packets. These protocols can include the unicast routing protocols such as RIP or OSPF, and the multicast protocols such as DVMRP or MOSPF. Normally routers communicate between each other to exchange status and routing information in order to optimize delivery of packets. This data exchange can include advertising routes the router is aware of to reach an end destination.

ROUTER LIMITATIONS

There are some physical implementation limitations in routers depending on the manufacturer and the model. For example in the Cisco 3600 series of routers, there is a maximum of 7000 entries allowed by default in the multicast routing table. Configuring the router can change this parameter.

Thus, in the Internet Protocol network, having a publicly available communications address is problematic as undesirable third parties may launch an attack, overwhelming the particular address or monitor the address for information not intended for the third party.

Transmitting IP packets to an IP address is somewhat akin to transmitting a radio signal at a particular frequency. A third party to the communication can monitor the frequency to eavesdrop on the communication or attempt to overwhelm or jam the frequency with a jamming signal. In the radio communications field, a technique known as spread spectrum communications employs a frequency hopping system where a transmitting station transmits bursts of data sequentially on a prearranged set of channels in a predetermined random pattern at specific times. The receiving station listens to the appropriate channels at the appropriate time in order to receive the communications. Frequencies can be shared among many users, as there can be many groups all hopping around in the frequency channels in a coordinated fashion. Spread spectrum techniques permit secure communications, reducing information gathering and denial of communications abilities. However such techniques require coordinated efforts between transmitting and receiving parties.

Thus, it is desirable for end stations to be able to communicate in an IP network having the limitations described herein, particularly where the address for communication is publicly known, having a method or system to alleviate most or all of the effects of certain types of Denial of Service attacks or information gathering.

SUMMARY OF THE INVENTION

The present invention provides a method and system for Internet Protocol network communications and a use thereof for protecting Internet sites

against denial of service and traffic analysis attacks on insecure public networks such as the Internet.

In an embodiment, the present invention provides a method for transmitting multicast packets between a transmitting end station and one or more receiving end stations, in a multicast IP network, on a chosen multicast IP address from a plurality of multicast IP addresses for multicast communication using a multicast address hopping technique. The technique selectively varies the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the end stations but not to unauthorized end stations. The packets are then communicated on the chosen multicast IP address. In an aspect of the invention, indicia normally capable of identifying the source of the packets may be selectively varied to conceal the source of the packets.

In another embodiment, there is provided a method for receiving multicast packets from a transmitting end station on a chosen multicast address from a plurality of multicast IP addresses for multicast communication using a multicast addressing hopping technique and where indicia normally capable of identifying the source of the packets may be selectively varied to conceal the source of the packets. The packets may be communicated to an end station having subscribed to a set of multicast IP addresses comprising at least one multicast IP address from the plurality of multicast IP addresses for multicast communication and including the chosen multicast IP address for transmitting the packets. The set of multicast IP addresses may also be selectively varied according to a secret predetermined scheme known to the end stations, particularly by randomly adding to and dropping from the set of multicast IP addresses.

The invention provides protection from unauthorized personnel who may determine which address to disrupt or monitor for traffic between the end stations. Even if the unauthorized personnel can discover a particular multicast address chosen, addresses are dropped and new ones generated in a random fashion thus limiting the time in which the attacker can monitor packets or direct packets against an end station. Multiple sets of communicating groups all utilizing

the same address space can coexist such that their respective traffic is intermingled on the various addresses, making traffic analysis very difficult.

In an aspect of the invention, the indicia may be chosen from the Time To Live (TTL) field and the IP Source address of individual IP multicast packets. The TTL field may be randomly set (jittered) to prevent eavesdroppers from deducing the separate sources of a packet stream through correlation of the TTL fields.

The IP Source Address of multicast IP packets may be "spoofed", that is filled in with a false source address, which can be changed in a random appearing method. Random appearing spoofed IP addresses prevent eavesdroppers from determining the real source of the packets.

In another embodiment, a data coding scheme such as code division multiplexing may be employed on the individual multicast packets data fields to allow data for individual destinations to be mixed together in one packet that is multicast to a plurality of receivers. Each receiver then decodes its applicable data by passing the received multicast data field through the appropriate decoding scheme such as a code division de-multiplexing process.

In further aspects of the invention, various uses of the invention for Virtual Private Networks and other secure communication systems are also provided.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other features and advantages will be better understood from the following detailed description of the MAHT technique and of certain preferred embodiments of the invention with reference to the drawings, in which:

FIG. 1 is a schematic diagram showing the general architecture of a system using the multicast address hopping technique;

FIG. 2 is a schematic diagram showing the general conceptual architecture of an MAHT receiving device implementing a multicast address hopping technique;

FIG. 3 is a schematic diagram showing the general conceptual architecture of an MAHT transmitting device implementing a multicast address hopping technique;

FIG. 4 is a schematic diagram showing the general architecture of an enhanced VPN system using MAHT to provide protection against a traffic analysis attack;

FIG. 5 is a schematic diagram showing the configuration of an enhanced VPN using MAHT with spoofed IP address and IP in IP tunnels to provide protection against traffic analysis;

FIG. 6 is a schematic diagram showing the configuration of an enhanced VPN using MAHT with spoofed IP addresses and multiple IP in IP tunnels to provide protection against traffic analysis;

FIG. 7 is a schematic diagram showing an MAHT system transmitting multiple data streams to a plurality of MAHT receivers such that only authorized subscribers correctly receive a given data stream;

FIG. 8 is a schematic diagram showing an MAHT system using code division multiplexing to transmit data to a plurality of MAHT receivers; and

Fig. 9 is a schematic diagram showing an overview of the existing prototype test bed.

DETAILED TECHNICAL DESCRIPTION

The following are features of the MAHT technology to aid in anti DoS attacks and anti traffic analysis for communications between end stations on a public network:

data is communicated between the stations by multicast protocol having multicast addressing which hides a receiving station's actual IP address;

multicast address hopping prevents others from discovering and monitoring or attacking a particular multicast address;

indicia within the packets normally capable of indicating the source of the packets may be selectively varied to conceal the source of the packets. For example, TTL fields may be jittered to prevent traffic analysis by correlation of TTLs, and IP Source Addresses may be spoofed (with or without the use of IP Tunneling) to conceal the IP Source Address of the transmitting station;

unicast routes to the stations forming a VPN may be suppressed to avoid a unicast based attack on the stations;

data coding of packet data, such as by CDMA techniques, may be employed to make analysis difficult.

The MAHT can be implemented in various configurations to give protection against different types of threats. Configuration possibilities depend on the type of in place network infrastructure particularly the multicast routing protocol and IP packet filtering definitions.

Referring now to the drawings and more particularly to FIG 1., there is shown, in a schematic diagram form, the general architecture of a system that uses the MAHT to communicate within an Autonomous System of the Internet. The MAHT Receiver, Block 100, is connected to an Autonomous System, Block 104, of the Internet through Router 1, Block 106. The MAHT Transmitter, Block 102 is connected to the same Autonomous System through Router 4, Block 108. There is a plurality of routers interconnected together that form the Autonomous System router network, Block 104.

The MAHT Receiver, Block 100, subscribes to a set of multicast addresses, from the plurality of available multicast addresses in the Autonomous System, by sending the appropriate IGMP subscribe messages to Router 1, Block 106. The MAHT Transmitter, Block 102, encapsulates data in a multicast packet with an address known to be in the current set of multicast addresses to which the MAHT Receiver, Block 100, has subscribed. The data may comprise unicast IP packets destined for the MAHT Receiver, Block 100, or another site with which the

Receiver is familiar (e.g. a site to be protected from a Denial of Service attack) or other data.

Router 1, Block 106 communicates with the other routers within the Autonomous System, Block 104, to request delivery of any multicast packets in the set of addresses in current use by the MAHT Receiver, Block 100. The Routers use the standard multicast routing protocol in use within the Autonomous System, Block 104, to communicate, e.g. PIM-DM, DVMRP, MOSPF, etc. In the example illustrated in Fig. 1, the MAHT Receiver, Block 100, has subscribed to a set of addresses starting with 224.1.6.4 and including 229.5.34.21. The MAHT Transmitter, Block 102, transmits the encapsulated data in multicast packets having an address selected from the same set of multicast addresses. After a time, a further address is selected for communicating with the Receiver. These multicast packets are then routed through the Autonomous System, Block 104, by the plurality of routers to be ultimately delivered to the MAHT Receiver, Block 100. If the encapsulated data comprised unicast data, the original unicast packets may then be recovered and passed on as may be necessary.

The set of addresses used by the MAHT Receiver, Block 100, and the MAHT Transmitter, Block 102, includes at least one address and preferably a larger number of addresses. The size of the set may vary depending on the capacity of the Receiver to maintain the set and the expected ability of third parties who may be monitoring the Receiver's communications. By choosing a sufficiently large number of addresses, the Receiver cloaks the particular addresses actually used for communication among those addresses to which it subscribes while lessening the chances that a person monitoring the communications can determine meaningful information about the communications.

In a preferred embodiment, addresses may be dropped from the set of addresses and new ones added to the set from the plurality of available multicast addresses in an agreed upon synchronized change scheme between the MAHT Receiver and Transmitter. Addresses for the set of addresses and particular address selected for a period of time for actual communication are selected in a fashion that is not known to parties not intended to be capable of

receiving the data, such as by random selection according to a prescribed scheme known to the MAHT Receiver and Transmitter.

The duration of the subscription by the MAHT Receiver to any address or addresses from the set of addresses and the length of time that a particular address is selected for actual communication is preferably of random length. This random addressing scheme makes it difficult, if not impossible, for a remote attacker to determine which multicast address to attack to carry out a denial of service attack on the MAHT Receiver or which address to monitor for information gathering purposes as data may be spread over multiple addresses. While in the preferred example, the Receiver subscribes to multiple addresses at any one time, it is understood that the receiver may subscribe to the selected address for communication in sufficient time prior to its use, dropping the address upon termination of its use. However, such a method does not hide the selected address among a set of potential addresses, should a third party be monitoring the subscription traffic from the Receiver.

Preferably, when the MAHT is used for anti Denial of Service of a unicast-based service supplied from an end station (as described more fully below), Router 1, Block 106, (and any router adjacent to a MAHT receiver, Block 100, or transmitter Block 102) is configurable such that it does not advertise an IP route to itself nor to any downstream connected devices. This means that even though there is a physical communication link between itself and a neighboring upstream router., Router 2, Block 110, or Router 5, Block 112, the upstream router is not aware of the address of the downstream router. However, the downstream router can still pass IP packets addressed to remote network hosts through the physical communication link to the upstream router that forwards them on to the remote hosts. This in effect leaves a one-way unicast route from the downstream router, e.g. Router 1, Block 106, and any connected downstream hosts, e.g. the MAHT Receiver, Block 100, into the Internet. No unicast packets can be delivered to the downstream router, e.g. Router 1, Block 106, or connected hosts, e.g. the MAHT Receiver, Block 100, since there are no unicast routes available to route them from the upstream router e.g. Router 2 or Router 5. This means that no

attack packets can be directed against the router or protected host since no route exists to them. The ability to configure a router in this mode is a built in capability to most commercial routing equipment.

It is understood that for multicast protocol within the IP network, routers, e.g. Router 1, Block 106, permit multicast subscribe or de-subscribe (IGMP) packets to be passed from the downstream router, Router 1 to the upstream router through the physical communication link connected to the applicable interface. The upstream router e.g. Router 2 or Router 5, receives these IGMP subscribe or de-subscribe messages on the interface corresponding to the physical communication link to the downstream router, e.g. Router 1. This upstream router will then become aware that there is a multicast subscriber for that particular multicast address somewhere through that interface even though the router is not aware of the addresses of any hosts or subnets reachable through that interface. The upstream router, e.g. Router 2 or Router 5, then processes a request through to the other routers within the Autonomous System to receive any packets destined for that multicast address. When the router receives these multicast packets from senders elsewhere within the Autonomous System, Block 104, e.g. the MAHT Transmitter, Block 102, it will forward these multicast packets through the interface to the downstream router, e.g. Router 1, Block 106. In this example, Router 1, Block 106, will then pass these multicast packets on to the MAHT Receiver, Block 100. The ability to configure a router in this mode is a built-in capability to most commercial routing equipment.

Referring now to FIG. 2, there is shown a representative schematic diagram of a general conceptual architecture for a MAHT Receiver implementing the multi address hopping technique for receiving data from a MAHT Transmitter. The MAHT Receiver, Block 200, could be built as a specialized device or run as a software program on a general- purpose computer.

The MAHT Receiver, Block 200, includes a multicast address generating function comprising means to selectively vary the choice of multicast addresses on which to receive multicast data from the plurality of available multicast addresses for communicating with another end station. The Receiver

further comprises means to synchronize with the Transmitter for coordinated communication on the selected multicast addresses. In the preferred embodiment, the means to selectively vary the choice of addresses comprises means to generate addresses according to a secret predetermined scheme known to the Receiver and a Transmitter, which means may be initiated by a cryptographic key. The predetermined scheme is secret in that it may be known by the Receiver, Transmitter and other selected end stations but not by another who may wish to monitor or disrupt the traffic of the selected end stations.

The MAHT Receiver, Block 200, may be connected into the IP based public network (e.g. Internet) through one or more interfaces such as an Ethernet port shown at Block 202. Configuration File, Block 204, and a current Cryptographic Key, Block 206, contain the necessary information to initialize and start the MAHT. The Configuration File may include such things as number of active Wide Area Network, (WAN), multicast ports to open, cryptographic algorithms to use, and logging settings. The System Initializer process, Block 208, reads in the Configuration File, Block 204, and the current Cryptographic Key, Block 206, and then creates the other processes with the appropriate parameters. Listen Address Generator, Block 210, generates the appropriate multicast addresses to listen to in accordance with the predetermined scheme and any configuration parameters. These parameters include the current time, number of addresses to open, and current cryptographic key. The Time Synchronization process, Block 212 provides the current time to the Listen Address Generator, Block 210, so that the addresses are subscribed to and dropped in synchronization with the remote MAHT Transmitter. The time synchronization could be based on the system clock, an externally supplied more accurate time standard, e.g. from a Global Positioning Satellite receiver, a network time standard such as the Network Time Protocol (NTP), or a time synchronization method with the MAHT process potentially based on the NTP technique for synchronizing time across an IP network.

The WAN Listener processes, (Block 214 through 218), are created by the Listener Address Generator, Block 210. The number of WAN Listener processes created is determined by the configuration file parameters, Block 204. Each of these WAN Listener processes will listen to a different multicast address by subscribing to the upstream router using an IGMP subscribe packet sent through the Ethernet port, Block 202. Each WAN Listener process will drop their current address and subscribe to a new one in accordance with the control signals from the Listen Address Generator, Block 210. Each WAN Listener, Block 214 through 218 passes any received multicast packets to the Packet De-encapsulator, Block 220.

The Packet De-encapsulator takes the data, for example a unicast packet, from the multicast packet and performs any checks or processing on the packet including decryption and authentication if so configured. Packets are checked to ensure that they actually originated with the appropriate MAHT Transmitter. If they are actually from another multicast transmitter using the same address, these packets are discarded. If the multicast packet is from the appropriate MAHT Transmitter and the data is a unicast packet intended for a host site familiar to the MAHT Receiver, Block 200, the Packet De-encapsulator, Block 220, may pass the de-encapsulated unicast packet on to the LAN Transmitter, Block 224, to send the packet out through the Ethernet Port, Block 202, in its original unicast format, to be delivered to the unicast destination host.

Optionally, in the preferred embodiment, the processing of packets in the Packet De-encapsulator is monitored by the Collision Detection process, Block 222. This process determines if there are too many packets arriving on a multicast address that are actually from another multicast transmitter using the same address, in effect an address collision. If there is too much traffic on this address then the Collision Detection process, Block 222, can instruct the Listen Address Generator, Block 210, to drop this particular address and add a new one before the normal scheduled address drop time. The remote MAHT Transmitter can be notified that this particular address has been dropped via a control packet sent from the MATH Receiver, Block 200, to the MAHT Transmitter.

Referring now to FIG. 3, there is shown a representative schematic diagram of a preferred architecture for a MAHT Transmitter, Block 300, implementing the multicast address hopping technique for transmitting data to a MAHT Receiver. The MAHT Transmitter, Block 300, could be built as a specialized device or run as a software program on a general purpose computer.

The MAHT Transmitter, Block 300, includes a multicast address generating function comprising means to selectively vary the choice of multicast addresses on which to transmit multicast data from the plurality of available multicast addresses for communicating with another end station. The MAHT Transmitter, Block 300, further comprises means to synchronize with the MAHT Receiver for coordinated communication on the selected multicast addresses. In the preferred embodiment, the means to selectively vary the choice of addresses comprises means to generate addresses according to the secret predetermined criteria known to the MAHT Receiver and the MAHT Transmitter, which means may be initiated by a cryptographic key as described herein above. The MAHT Transmitter may be connected into the Internet through one or more interfaces such as an Ethernet port shown at Block 302.

Configuration File, Block 304, and a current Cryptographic Key, Block 306, contain the necessary information to initialize and start the MAHT Transmitter, Block 300. The Configuration File may include such things as number of WAN multicast addresses to use, information for cryptographic steps, TTL jitter settings, IP spoofing settings, Retransmit Servers to use, and logging settings. The System Initializer process, Block 308, reads in the Configuration File and the current Cryptographic Key and then creates the other processes with the appropriate parameters.

For the case where the MAHT Transmitter, Block 300, is used to forward unicast data received from another host to the MAHT Receiver or a host with which the MAHT Transmitter and Receiver are familiar, LAN Listener process, Block 318, listens for appropriate unicast packets received on the Ethernet port,

Block 302. The LAN Listener process, Block 318, then passes these packets on to the Packet Encapsulator, Block 316.

The Packet Encapsulator, Block 316, takes the original unicast packet from the LAN Listener process, Block 318, and performs processing on the packet including encryption and authentication, if so configured, to build a multicast packet. In other cases, the Packet Encapsulator may encapsulate and process other data it receives from other processes (not shown). The Transmit Address Generator, Block 310, generates the appropriate multicast addresses to transmit to in accordance with the configuration parameters. These parameters include the current time, number of addresses to use, hopping order, and current cryptographic key. The Time Synchronization process, Block 312 provides the current time to the Transmit Address Generator, Block 310 in accordance with a method discussed in relation to the Receiver, so that the addresses for transmission are selected and dropped in synchronization with the MAHT Receiver.

The TTL field is a mechanism used in IP packets to ensure packets do not loop endlessly around a network without ever reaching their destination. The TTL data field in an individual IP packet is decremented every time it passes through a router or spends a predetermined time (e.g. 30 seconds) waiting in a queue. Once the TTL field in a packet reaches 0 the router that is handling it automatically discards the packet. The maximum value of TTL is 255 but can be set lower to limit the hops a packet can travel. Setting the TTL to a low value to prevent distant travel is known as administrative scoping and is often used to limit how far multicast packets can travel. The Packet Encapsulator may set the Time To Live (TTL) field in individual IP multicast packets randomly (i.e. in a jittered manner) to prevent eavesdroppers from deducing the separate sources of a packet stream through correlation of the TTL fields. Of course, the value chosen should not be so low as to prevent reception of the packet by the intended receiving station. In a preferred embodiment, the TTL value is jittered around a nominal average value that is chosen such that the maximum range of jitter to be added and subtracted from the nominal average value will not be so low as to

prevent reception of the packet by the intended receiving station nor so high as to be beyond the maximum value of 255. The average TTL value could be chosen depending on network topology and any administrative scoping requirements. The generated jitter values would preferably be in a uniform distribution for values to produce the maximum and minimum acceptable values of TTL. For example, the nominal TTL could be set to 128 with a uniform distribution for the generated TTLs from a minimum of 64 to a maximum of 192. The system could be further enhanced by including an adaptive process such that the individual nominal average TTL values are adaptively set so that the average TTL values arriving at a receiving site are adaptively adjusted to be the same for different transmitting sites. This adaptive process requires feedback from the MAHT receiving sites to the MATH transmitting sites. This adaptive process would further complicate any traffic analysis attempts by hiding any differential trends in average TTL for packets originating from different transmitting sites.

WAN Transmitter process, Block 314, is created by the Transmit Address Generator, Block 310. The WAN Transmitter receives encapsulated packets from the Packet Encapsulator, Block 316, and transmits them to the Internet through the Ethernet port, Block 302. Optionally, The MAHT Transmitter, Block 300, can be notified that a particular multicast address has been dropped, due to address collision, via a control packet sent from the MAHT Receiver to the MAHT Transmitter.

The MAHT may work with any of the IGP multicast routing protocols within an Autonomous System. Once an EGP, such as BGMP, has been defined and implemented the present invention can operate across Autonomous Systems. It is also currently possible to use well-known IP tunneling techniques to communicate multicast packets between two autonomous systems although this is an administration intensive process.

The MAHT does not necessarily require scoping but can use either TTL, administrative, or both types of scoping methods to increase the effectiveness of the system or to meet administrative requirements.

The MAHT can work within the developmental Multicast Address Allocation architecture provided that the total number of multicast addresses available is sufficient and the allocation order can be randomized in some fashion. Until the dynamic address allocation problem is resolved and standardized the present invention can operate within an Autonomous System by defining it's own multicast addresses and ensuring detection and handling of packets from other applications using the same multicast address. If there is an address collision such that there are too many erroneous packets being delivered then that particular address can be dropped.

Physical router limitations, especially the simultaneous number of open multicast route entries, must be taken into account when planning and implementing this invention in a particular Autonomous System of the Internet. These limitations can impact the implementation configuration of the present invention. However routers typically have a default limit of several thousands of routes and can be configured for more if required. For example, the Cisco 3600 series of routers have a default limit of 7000 multicast route entries that is expected to be more than adequate for practical implementation of this invention.

The MAHT may be used in a system and method for protection against certain types of Denial of Service attacks for Internet sites using IP networks, especially the Internet, as a communications media.

In one embodiment, the system can provide anti-traffic analysis capabilities for communications between a site and a number of other sites. Referring now to Figure 4, there is shown a system that has a transmitting site and a number of receiving sites. The transmitting site, Block 400, uses the MAHT technique to transmit traffic to the plurality of receiving sites, Blocks 402, 404, and 406. Any attacker, Block 408, who monitors the transmitted packets, does not know to whom the packets are really destined thus denying him destination information to analyze. Notethat under normal multicast transmission schemes, the attacker does know from where the packets originated by observing the source address in the multicast packet.

Depending on which multicast routing protocol is in effect in the Autonomous System, it may be possible to spoof the IP Source address for the multicast packets. Spoofing in this case means randomly putting in a false address for the IP Source address in the IP Source address field of the packet. This would deny the attacker knowledge of the source of the packets. Implementation of the IP Address Spoofing technique is straightforward for use with the Core Based Tree (CBT) multicast routing. The Packet Encapsulator, Block 316, of a transmitting end station may insert a spoofed IP Source Address, unconnected to the transmitting end station, in the multicast packet.

Spoofing the source address may have practical implementation aspects involving filtering at routers in the Internet and in the multicast routing protocol in use in the Autonomous System. Certain multicast routing algorithms, notably the Distance Vector Multicast Routing Protocol (DVMRP), cannot easily be used with IP spoofing techniques. This is due to the fact that they use a reverse path forwarding technique for multicast packets whereby a multicast packet is only forwarded on to other subscribing routers only if the packet is received on the physical interface through which a unicast packet destined for the source address in the multicast packet would be sent. The implementation configuration of the MAHT with spoofed IP addresses depends on which multicast routing protocol is in effect in the implementation area. For example, use of MAHT including IP spoofing in a DVMRP area will require use of additional infrastructure or techniques such as IP tunneling.

Referring now to Figure 5, there is shown a MAHT system that uses tunnels to allow IP spoofing to protect the IP Source address of the transmitting site. The Transmitting site, Block 500, takes the multicast packet and encapsulates it in a tunneling protocol such as IP in IP. The multicast packet has a spoofed IP Source address inserted in place of the normal IP Source address. The multicast packet is encapsulated in a unicast tunnel packet, Block 502. This unicast tunnel packet also has a spoofed IP Source address. This unicast packet is then delivered into the Internet to be delivered to the receiving tunnel exit host or router system, Block 504, at the other end of the tunnel. Once this unicast

packet arrives at the other end of the tunnel the multicast packet is de-encapsulated and processed as a normal packet. By appropriate selection for the spoofed IP Source address in the multicast packet, the underlying multicast routing protocol will correctly process this de-encapsulated packet at the tunnel exit host and deliver it to the receiving site, Block 506. In this way the transmitting source address can be hidden from attackers. Preferably there is a plurality of tunnels implemented leading to a plurality of tunnel exit hosts thereby greatly increasing the complexity of any attacker traffic analysis and also providing greater reliability and anti denial of service capability. This plurality of exit hosts could be scattered throughout an Autonomous region or across several Autonomous Systems, thus ensuring multiple widely separated paths for the data packet flow.

Referring to Figure 6, there is shown a system incorporating multiple tunnels scattered across an Autonomous Region. There is an MAHT transmitting site, Block 600, that encapsulates the original multicast MAHT packets with a spoofed IP Source address, Block 602, 604, and 606 in unicast tunnel packets addressed to the range of tunnel exit hosts, Blocks 608, 610, and 612. Any encapsulated multicast packet arriving at a tunnel host will be de-encapsulated and delivered using the standard underlying multicast routing algorithm to the MAHT receiving sites, Blocks 614, 616, and 618. Note that the multicast packets exiting from the IP in IP tunnel can be destined to a plurality of MAHT receivers. The capability of the tunneling technique could be further enhanced over the standard IP tunneling techniques such as IP in IP by adding custom software to the tunnel exit hosts and the MAHT transmitter such that the packets are encrypted thus providing even greater resistance to traffic analysis.

In another embodiment, the MAHT can provide anti denial of service capabilities to a VPN system. In this embodiment, the VPN sites across the public network are all configured to use the MAHT technique to communicate on a full time basis. The VPN is set up such that there is no return unicast route from the public network back into the MAHT configured VPN sites. Such a requirement may be met by the non-advertisement of a unicast route to the VPN sites, by filtering unicast packets destined for the sites or decoying unicast traffic to another

device. The MAHT technique allows the data traffic to flow between the various communicating sites but denies an attacker an effective unicast IP address against which to direct a denial of service attack. Preferably this embodiment would also include varying the indicia of packet source, such as the use of the IP spoofing techniques previously described, in order to provide anti traffic analysis capabilities as well.

In another embodiment, the MAHT system could be set up to provide an emergency backup mode for individual VPN sites that come under active denial of service attacks. In this embodiment, the individual VPN sites would normally communicate with default unicast point to point protocols. However if one site came under active denial of service attack then it could switch either manually or, preferably, automatically, to MAHT back up mode. In this mode the router connecting the VPN into the public network would be instructed, preferably by the VPN device using an automatic control channel, to cease advertising a unicast route into the site, thus shutting down the denial of service attack. The VPN site would then commence using the MAHT technique to communicate to the other VPN sites. The site under attack instructs the other VPN sites to transmit to it using MAHT. As the site under attack is still capable of unicast transmission even though unicast reception is suppressed, the site could still use normal unicast to send packets to the other VPN sites. Otherwise, the site under attack may indicate to the other VPN sites a desire to transmit to them using MAHT. Once the attack has ceased or been isolated then the VPN site under attack could revert back to normal operation.

In another embodiment, the MAHT system could be used to deliver data streams to multiple authorized receivers while providing an efficient method to prevent unauthorized users from viewing the data. It is computationally costly to perform real time high bandwidth decryption and administratively difficult to distribute decryption keys to multiple subscribers. Rather than encrypting the data stream it would be more efficient to use the MAHT technique to transmit the data stream on different and changing multicast ports. The receiving subscribers would have to know the correct hopping sequence and timing but would not be required

to run any real time decryption software or hardware. It is computationally trivial to subscribe and de-subscribe to multicast addresses. The receiving subscribers could receive the hopping sequence through various means. For example, a subscriber could establish a secure connection to a web site using a standard protocol like Secure Sockets Level, (SSL). This web site would provide a pay for use service by passing through this connection the hopping sequence and timing to the end user on a continuing basis and the user could be charged on the basis of the time connected to the hopping and timing server and which data stream was used. Alternately, a user could receive the appropriate sequence and timing information for a fixed period for a periodic fee. This service would preferably offer multiple different data streams, for example, video (movies), audio (radio broadcasts), or real time data (stock quote feeds). This would increase the difficulty for an unauthorized user to effectively intercept the correct data stream.

Referring now to Figure 7, there is shown a MAHT system transmitting multiple data streams to a plurality of MAHT receivers such that only authorized subscribers correctly receive a given data stream. The MAHT transmitter, Block 700, receives a plurality of data streams, for example video streams, Blocks 702, 704, and 706, from connected sources, 708, 710, and 712. The MAHT transmitter, Block 700, uses the MAHT technique to transmit these data streams in MAHT multicast packets to multiple and changing multicast addresses in the Internet, Block 714. Authorized users, Blocks 716, 718, and 720, who have the correct addressing hopping and timing sequence for a given data stream can subscribe to the appropriate address at the appropriate times and receive the data stream. In this case Authorized Subscriber 1, Block 716, has subscribed to Data Stream 2, Block 704, and similarly Authorized Subscriber 2, Block 718, to Data Stream N, Block 706, and Authorized Subscriber N, Block 720, to Data Stream 1, Block 702. If a subscriber does not have the correct information they will not receive the packets correctly and may even receive a mixed up conglomeration of packets originating from different data streams.

In another embodiment, the system may be further enhanced by formatting a data portion of the multicast packet with data intended for different end stations according to a data coding scheme for combining and separating the data. The scheme may use a code division multiplexing technique. In a preferred embodiment of this system, a MAHT Transmitting site communicates with a plurality of MAHT Receiving sites using the MAHT technique. However each Receiving site subscribes to the same full set of multicast addresses and therefore receives all packets communicated. However, the MAHT transmitting software uses a code division multiplexing algorithm to embed data for every site on every packet, including null data if there were no data for a particular receiving site. An IP packet typically consists of an IP packet header, header options (if needed) and a data or payload portion. The data portion itself can be divided into a header and data depending on what protocol is being used for that packet. It is intended that the code division multiplexing process be used on the portions of the IP packet not including the actual IP packet header.

Code division multiplexing or direct sequence spreading is a well-understood and implemented technology. In this embodiment, a different orthogonal code sequence having a fixed length is generated for each receiving end station. After a given number of bits the orthogonal code repeats itself exactly. In classic direct spreading the speed of the code sequence is called the chipping rate, measured in chips per second (cps). In this invention, it is called a chip ratio, since the underlying physical network, that may change during transit, determines the speed at which the bits or chips are transmitted on each segment of the physical communications link. For direct sequence, the amount of spreading is dependent upon the ratio of chips per bit of information. Each bit of the original message is multiplied by the code sequence thus the original message is spread by the factor of the orthogonal code length. For example a 50 bit message that is spread with a 5 bit code will result in a 250 bit coded sequence. At the receiver, the information is recovered by binary multiplying the signal with a locally generated replica of the code sequence for each sequence of bits corresponding to the code length and counting the number of "one" bits in the result. The

resultant count is put through a threshold device to decide whether the original bit was a binary "one" or "zero". This process is sequentially used on each set of bits corresponding to the code length to recover the original sequence of bits in the message.

Referring now to Figure 8, there is shown a system using both MAHT and code division multiplexing. The MAHT transmitter, Block 800, sends different data to a plurality of MAHT receivers, Blocks 802, 804, and 806. A pseudorandom sequence generator, Block 808, generates a different orthogonal code sequence for each MAHT receiver, e.g. Block 810. The MAHT transmitter then takes the data destined for each receiving site, e.g. Block 812 destined for Receiver 1, and multiplies each bit in the message destined for that receiver by its corresponding code sequence, e.g. Block 810, to result in a combination data and code sequence for each receiver, e.g. Block 814 for Receiver 1, which is the length of the data length times the code sequence length. These individual data and code sequences are then arithmetically added together to result in a combined result, Block 816, containing data destined for all the receivers. Note that any carry over bits from this binary addition process are discarded. This data is then packaged in a data portion of an MAHT multicast packet and transmitted to all the MAHT receivers, Blocks 802, 804, and 806, that have all subscribed to the applicable multicast address to receive this packet.

Once the multicast packet is received at a given MAHT receiver the data destined for that particular receiver is recovered by passing the received combined result from the data portion of the packet, Block 818, through a code division de-multiplexer that uses the identical pseudorandom sequence, Block 822, that the MAHT transmitter used to encode the data for that receiver. The received combined data, Block 818, is identical to the Combined data at Block 816. The code division de-multiplexer consists of a pseudorandom sequence generator, Block 820, which generates the same sequence, Block 822, as the code sequence, Block 810, generated by the MAHT Transmitter pseudorandom generator, Block 808, for traffic destined for Receiver 1. The output of the de-multiplexer is the original data destined for Receiver 1. Such a system may be

further extended by having the spreading sequence be much longer than a physical packet length thus enabling more reliable delivery of data when packets are lost in transit since information could be recovered even if some packets are lost. It is also possible to implement this system in a full duplex arrangement between a plurality of participating sites by having each site run both the MAHT transmitting and receiving systems with the appropriate parameters. A Transmitting site may incorporate null data in the coding scheme for sites for which there is no current data to be sent.

As may be understood, a data coding scheme such as code division multiple access may be used in a multicasting network protocol that does not incorporate MAHT or that does incorporate MAHT with schemes to hide the source of the multicast packets, such as TTL jittering or IP Source Address.

The MAHT of the subject invention has been partially prototyped and tested using a three router laboratory test bed. Referring now to Figure 9, there is shown the set up for the existing prototype test bed. The test bed comprised two Cisco™ 3620 model routers, Router 1, Block 908, and Router 2, Block 910, directly connected together using DCE and DTE V.35 cables. These directly connected cables simulated a long distance high- speed serial communications link. Each of these Cisco Routers was connected in turn through one of their Ethernet ports to a Local Area Network (LAN), LAN 1, Block 906, for Router 1, and LAN 2, Block 912, for Router 2. There was an Intel™ based Linux ™ computer, Block 904, running custom software developed for the MRS functionality located on LAN 1. This MRS computer had a second Ethernet card that connected to LAN 3, Block 902, and was configured to route IP packets between the LAN 1, and LAN 3. There was a Linux computer used as a Protected Server Site Host, Block 900, which was also connected into LAN 3, Block 902. This PSSH Linux workstation was configured to run an ftp server, an http server, a telnet server, and an email server. On LAN 2, Block 912, there were two computers connected, a Linux based workstation, Block 914, and a Windows™ 95 based workstation, Block 916. The Linux based workstation, Block 914, was running custom software to provide DFS functionality. The Windows computer, Block 916, was running a Netscape™ and

Microsoft Internet Explorer™ web browser software as well as standard Windows ftp, ping, and telnet client software.

Router 1, Block 908 was configured to block all packets destined for the PSSH, Block 900, that arrived on the serial interface from Router 2, Block 910. However, the Routers were configured using the Protocol Independent Multicast – Dense Mode (PIM-DM) routing protocol to allow multicast packets to travel from the rest of the network to LAN 1, block 906 and LAN2, Block 912. Thus there was a multicast route available between LAN 1 and LAN 2 but no unicast traffic was allowed to flow from the Client Host, block 916 to the PSSH, Block 900.

The system was tested using ftp, ping, web browsing, and ping between the PSSH and Client Host. When the DFS software, Block 914, and MRS software, Block 904 were turned off there was no connectivity between the Client Host and the MRS. When the DFS and MRS were turned on thereby initiating the MAHT protocol, then normal communications occurred between the Client Host and the PSSH using ftp, telnet, ping, and web browsing. The DFS, Block 914, picked up packets destined for the PSSH, Block 900, using packet sniffing software, encapsulated them in multicast packets, and sent them back to Router 2, block 910. This router forwarded the packets out its serial interface 0/1 to Router 1, Block 908, since Router 1 had been receiving IGMP subscribe messages for each of the 20 multicast addresses. These packets were delivered to the MRS, Block 904, where the original unicast packets were de-encapsulated and passed to the PSSH, Block 900, through the second Ethernet interface onto LAN 3, Block 902. Normal unicast packets from the PSSH, Block 900, destined for the Client Host, Block 916, could still pass normally from the PSSH through the network to the Client Host. This allowed a full bi-directional flow of data between the PSSH, Block 900 running various services and the Client Host, Block 916, in a completely transparent manner. The system achieved a rate of over 80 kilo bits per second even while using 446 bit encryption on each packet.

The multicast address hopping software was implemented primarily in the Java™ programming language with several low level Ethernet packet interface routines implemented in the C language. The software was configured

to hop within a set of 20 multicast addresses in a fixed pattern and did not drop or add new addresses.

Although the present invention has been described with respect to certain preferred embodiments thereof, various changes and modifications may be suggested to one skilled in the art and it is intended that the present invention encompass such changes and modifications as fall within the scope of the appended claims

WHAT IS CLAIMED IS:

1. In a multicast capable Internet Protocol (IP) network, a method for transmitting multicast packets between a transmitting end station and one or more receiving end stations on a chosen multicast (IP) address from a plurality of multicast IP addresses for multicast communication, the packets comprising one or more indicia normally capable of identifying an end station as the source of the packets, the method comprising the steps of:

selectively varying the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the transmitting and receiving end stations;

selectively varying one or more of the indicia within the packets so as to conceal the source of the packets; and

transmitting the packets on the chosen multicast IP address.

2. The method of claim 1 wherein the step of selectively varying the chosen multicast IP address comprises:
randomly hopping from one multicast IP address to another.

3. The method of claim 1 wherein the indicia are chosen from the group comprising a Time To Life (TTL) field and a IP Source Address field of the multicast packets.

4. The method of claim 1 further including the step of tunneling the multicast packets according to a network protocol to one or more tunnel exit hosts each capable of receiving and re-transmitting the multicast packets.

5. The method of claim 1 further comprising the steps of:
combining according to a data coding scheme data intended for each receiving end station, at least some of the data being different for different receiving end stations, to make combined data capable of separation by each receiving end

stations to obtain the data intended for the receiving end station; and coding a portion of said packets for transmission to all receiving stations with said combined data.

6. The method of claim 5 wherein said data coding scheme is a code division multiple access (CDMA) scheme.

7. The method of claim 1 wherein the multicast packets comprise at least one stream of data and wherein the step or transmitting comprises, for each stream, transmitting the multicast packets comprising the stream to one or more receiving end stations.

8. In a multicast capable Internet Protocol (IP) network, a method for receiving multicast packets at one or more receiving end stations from a transmitting end station on a chosen multicast (IP) address from a plurality of multicast IP addresses for multicast communication, the packets comprising one or more indicia normally capable of identifying an end station as the source of the packets, the method comprising the step of:

selectively varying the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the transmitting and receiving end stations;

subscribing to the chosen multicast IP address; and

receiving the packets on the chosen multicast IP address;

wherein the one or more of the indicia within the packets are selectively varied so as to conceal the source of the packets.

9. The method of claim 8 further including the step of subscribing to a set of multicast IP addresses comprising at least one multicast IP address from the plurality of multicast IP addresses for multicast communication and including the chosen multicast IP address for transmitting the packets.

10. The method of claim 9 further comprising the steps of selectively varying the set of multicast IP addresses to which at least one of the receiving end stations is subscribed according to a predetermined scheme known to the at least one receiving end station and transmitting end station and subscribing to the varied set.

11. The method of claim 10 wherein the predetermined scheme for selectively varying the set of multicast IP addresses comprises randomly adding to and dropping from the set of multicast IP addresses.

12. The method of claim 8 wherein the step of selectively varying the chosen multicast IP address comprises:
randomly hopping from one multicast IP address to another chosen from the set of multicast IP addresses.

13. The method of claim 8 wherein at least one of the receiving end stations is isolated from the network so as to prevent the reception of unicast packets.

14. The method of claim 8 further comprising the step of:
separating according to a data coding scheme combined data from data intended for each receiving end station, at least some of the data being different for different receiving end stations and coded in a portion of said packets for transmission to all receiving stations to obtain the data intended for the receiving end station.

15. The method of claim 14 wherein said data coding scheme is code division multiple access (CDMA) scheme.

16. In a multicast capable Internet Protocol (IP) network, a system for transmitting multicast packets between a transmitting end station and one or more receiving end stations on a chosen multicast (IP) address from a plurality of

multicast IP addresses for multicast communication, the packets comprising one or more indicia normally capable of identifying an end station as the source of the packets, the system comprising;

means for selectively varying the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the transmitting and receiving end stations;

means for selectively varying one or more of the indicia within the packets so as to conceal the source of the packets; and

means for transmitting the packets on the chosen multicast IP address.

17. The system of claim 16 wherein the means for selectively varying the chosen multicast IP address comprises:

means for randomly hopping from one multicast IP address to another.

18. The system of claim 16 wherein the indicia are chosen from the group comprising a Time To Life (TTL) field and a IP Source Address field of the multicast packets.

19. The system of claim 16 further including means for tunneling the multicast packets according to a network protocol to one or more tunnel exit hosts each capable of receiving and re-transmitting the multicast packets.

20. The system of claim 16 further comprising:

means for combining, according to a data coding scheme data intended for each receiving end station, at least some of the data being different for different receiving end stations, to make combined data capable of separation by each receiving end stations to obtain the data intended for the receiving end station; and coding a portion of said packets for transmission to all receiving stations with said combined data.

21. The system of claim 16 wherein the multicast packets comprise at least one stream of data and wherein the step or transmitting comprises, for each stream, transmitting the multicast packets comprising each stream to one or more receiving end stations.

22. In a multicast capable Internet Protocol (IP) network, a system for receiving multicast packets at one or more receiving end stations from a transmitting end station on a chosen multicast (IP) address from a plurality of multicast IP addresses for multicast communication, the packets comprising one or more indicia normally capable of identifying an end station as the source of the packets, the system comprising:

means for selectively varying the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the transmitting and receiving end stations;

means for subscribing to the chosen multicast IP address; and

means for receiving the packets on the chosen multicast IP address;

wherein the one or more of the indicia within the packets are selectively varied so as to conceal the source of the packets.

23. The system of claim 22 further comprising means for subscribing to a set of multicast IP addresses comprising at least one multicast IP address from the plurality of multicast IP addresses for multicast communication and including the chosen multicast IP address for transmitting the packets.

24. The system of claim 23 further comprising means for selectively varying the set of multicast IP addresses to which at least one of the receiving end stations is subscribed according to a predetermined scheme known to the at least one receiving end station and transmitting end station and means for subscribing to the varied set.

25. The system of claim 24 wherein means for selectively varying the set of multicast IP addresses comprises means for randomly adding to and dropping from the set of multicast IP addresses.

26. The system of claim 22 wherein the means for selectively varying the chosen multicast IP address comprises:
means for randomly hopping from one multicast IP address to another chosen from the set of multicast IP addresses.

27. The system of claim 22 wherein at least one of the receiving end stations comprises means for isolating the receiving end station from the network for preventing the reception of unicast packets.

28. The system of claim 22 further comprising the step of:
separating according to a data coding scheme combined data from data intended for each receiving end station, at least some of the data being different for different receiving end stations and coded in a portion of said packets for transmission to all receiving stations to obtain the data intended for the receiving end station.

29. The system of claim 28 wherein said data coding scheme is code division multiple access (CDMA) scheme.

Figure 1

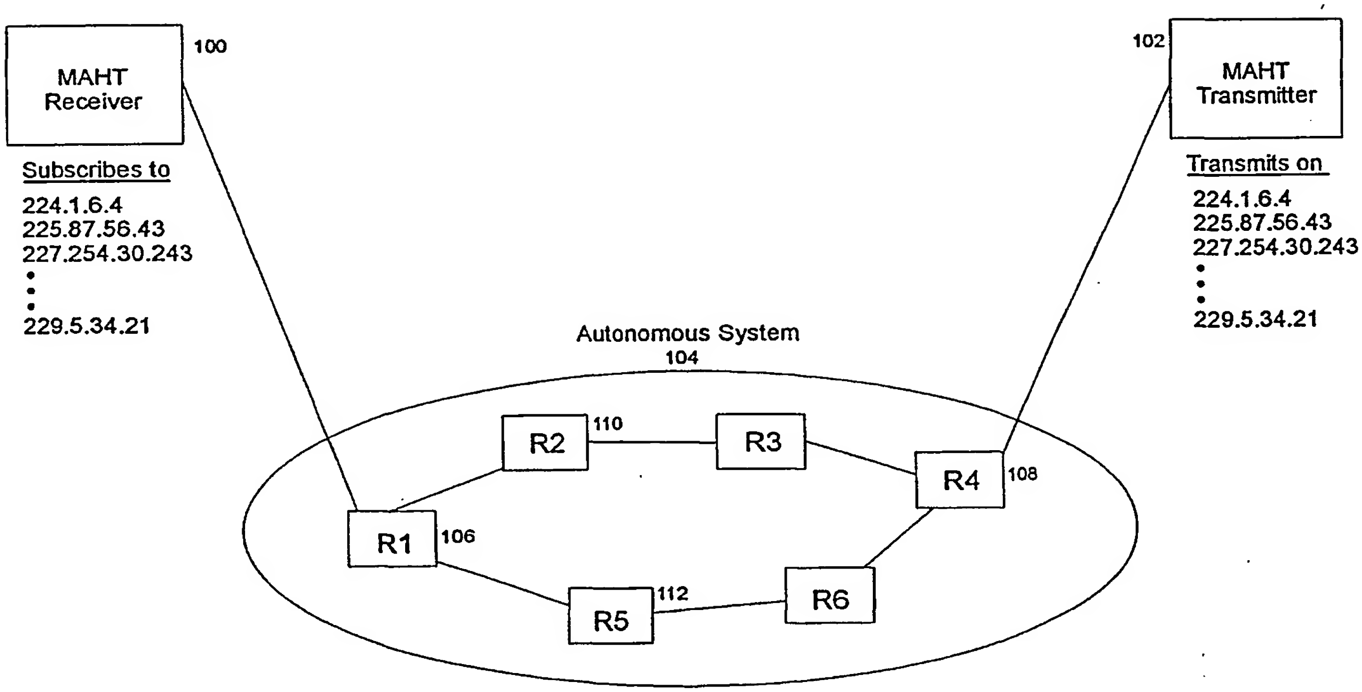

MAHT Receiver
100
Subscribes to
224.1.6.4
225.87.56.43
227.254.30.243
229.5.34.21
MAHT Transmitter
102
Transmits on
224.1.6.4
225.87.56.43
227.254.30.243
229.5.34.21
Autonomous System
104
R1
106
R2
110
R3
R4
108
R5
112
R6

Figure 2

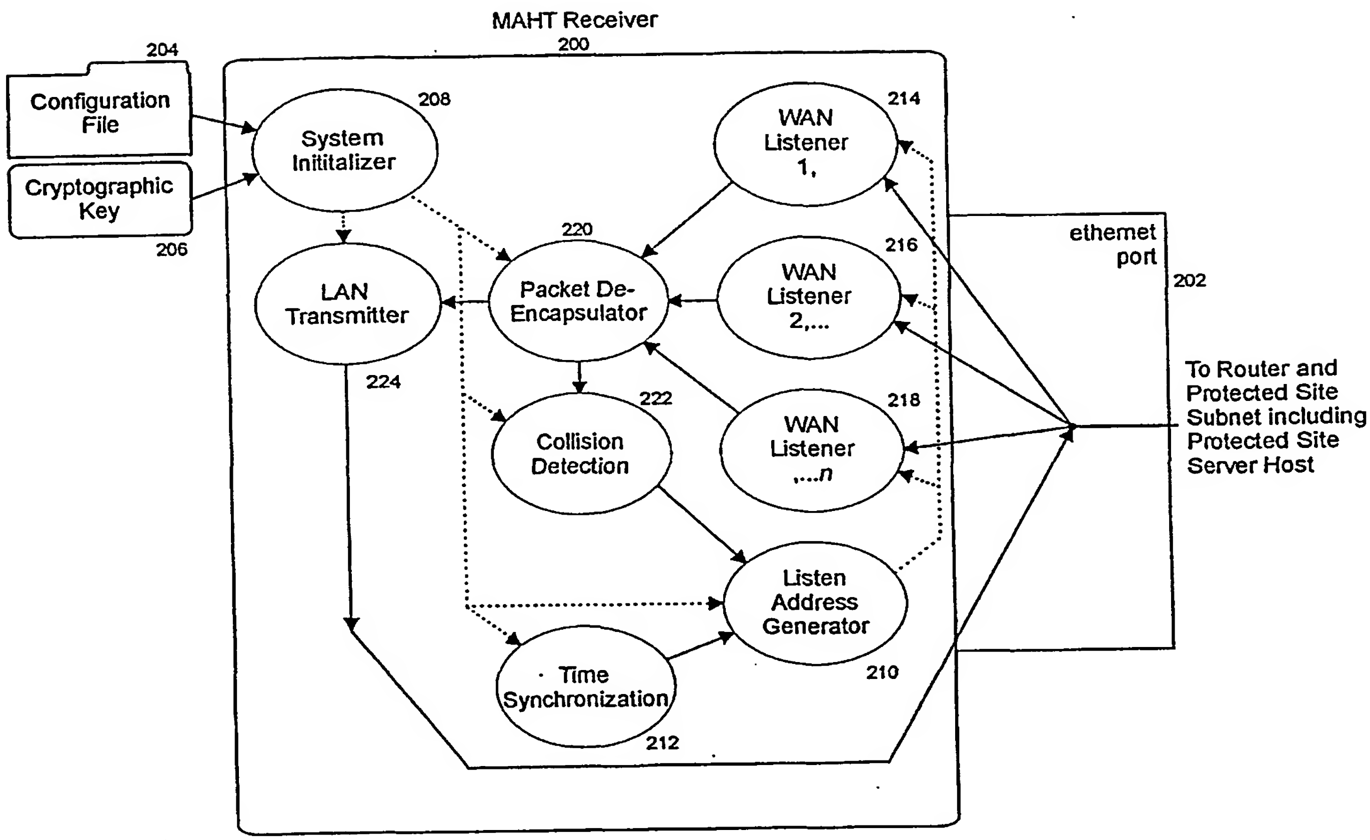

MAHT Receiver
200
204
Configuration File
Cryptographic Key
206
System Inititalizer
208
LAN Transmitter
224
Packet De-Encapsulator
220
Collision Detection
222
Time Synchronization
212
Listen Address Generator
210
WAN Listener 1,
214
WAN Listener 2,...
216
WAN Listener ,...n
218
ethernet port
202
To Router and Protected Site Subnet including Protected Site Server Host

Figure 3

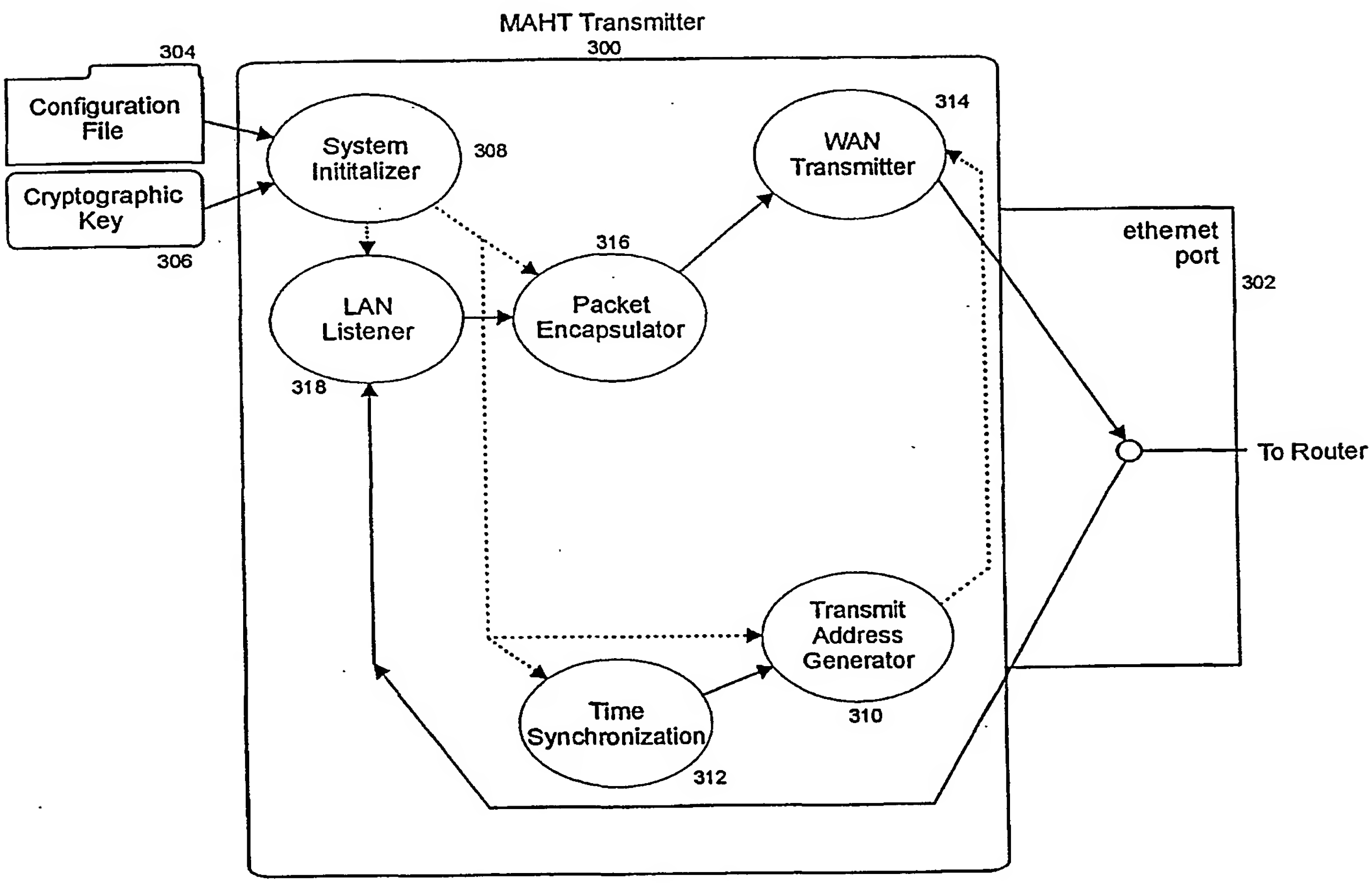

MAHT Transmitter
300
304
Configuration File
Cryptographic Key
306
System Inititalizer
308
LAN Listener
318
316
Packet Encapsulator
WAN Transmitter
314
ethernet port
302
To Router
Transmit Address Generator
310
Time Synchronization
312

Figure 4

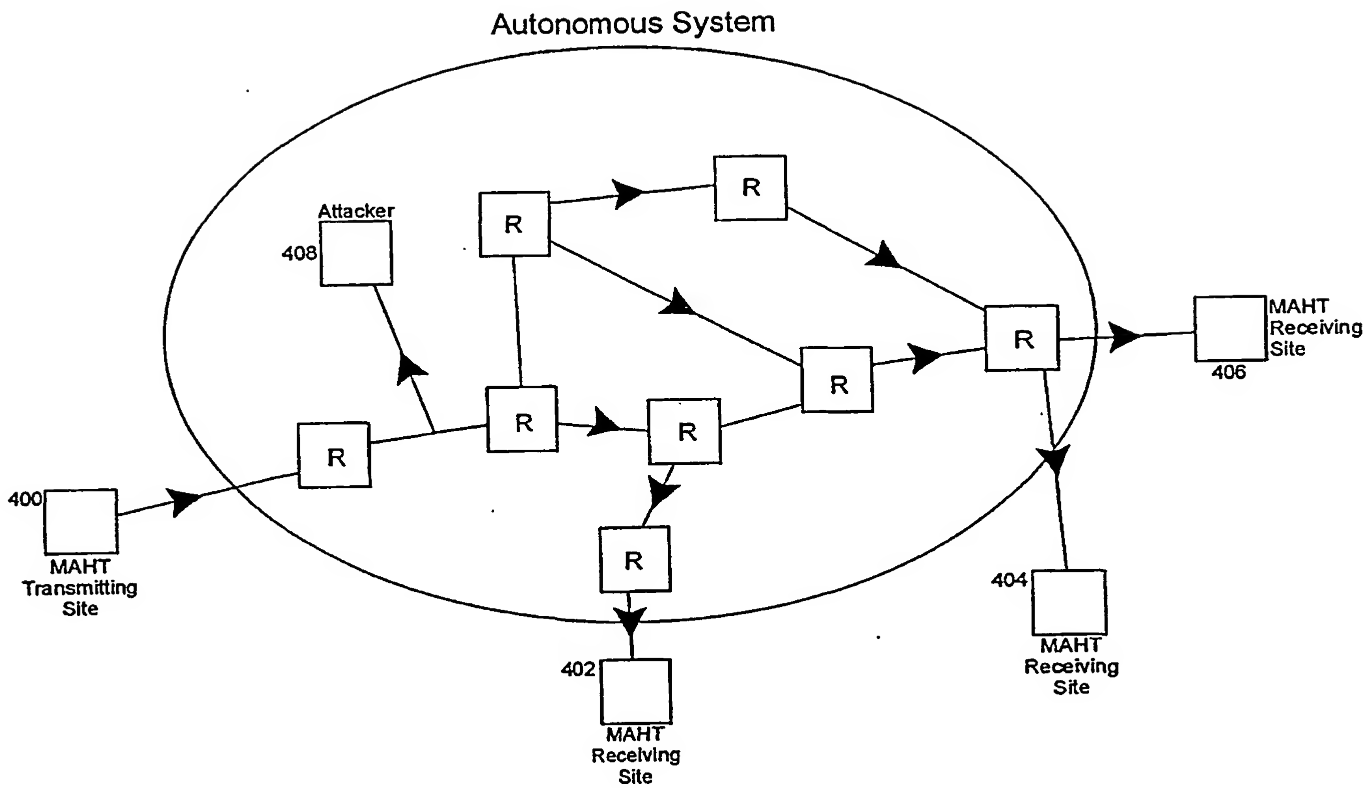

Autonomous System
Attacker
408
R
R
R
R
R
R
R
R
400
MAHT
Transmitting
Site
402
MAHT
Receiving
Site
404
MAHT
Receiving
Site
MAHT
Receiving
Site
406

Figure 5

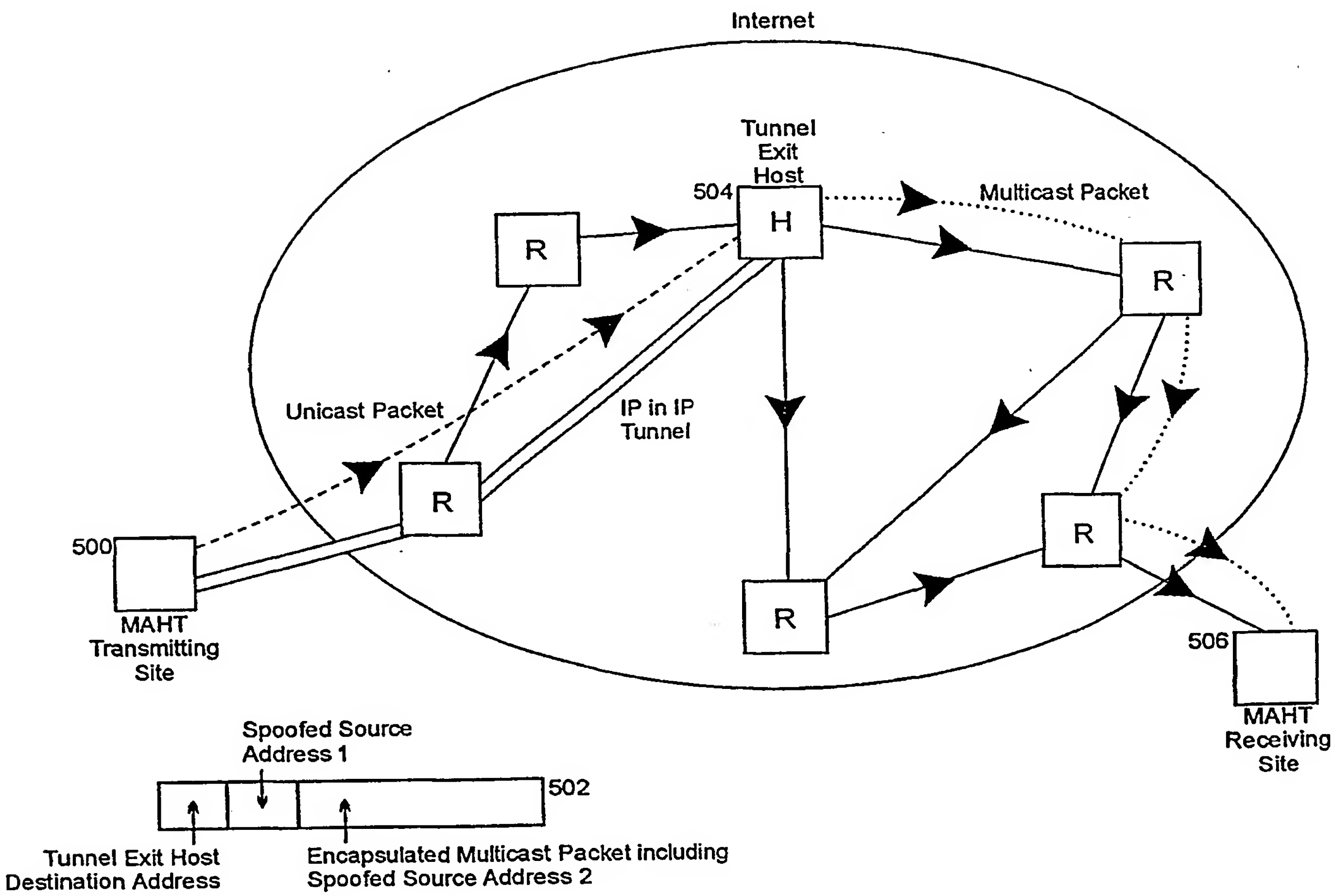

Internet
Tunnel
Exit
Host
504
H
Multicast Packet
R
R
Unicast Packet
IP in IP
Tunnel
R
R
R
500
MAHT
Transmitting
Site
506
MAHT
Receiving
Site
Spoofed Source
Address 1
502
Tunnel Exit Host
Destination Address
Encapsulated Multicast Packet including
Spoofed Source Address 2

Figure 6

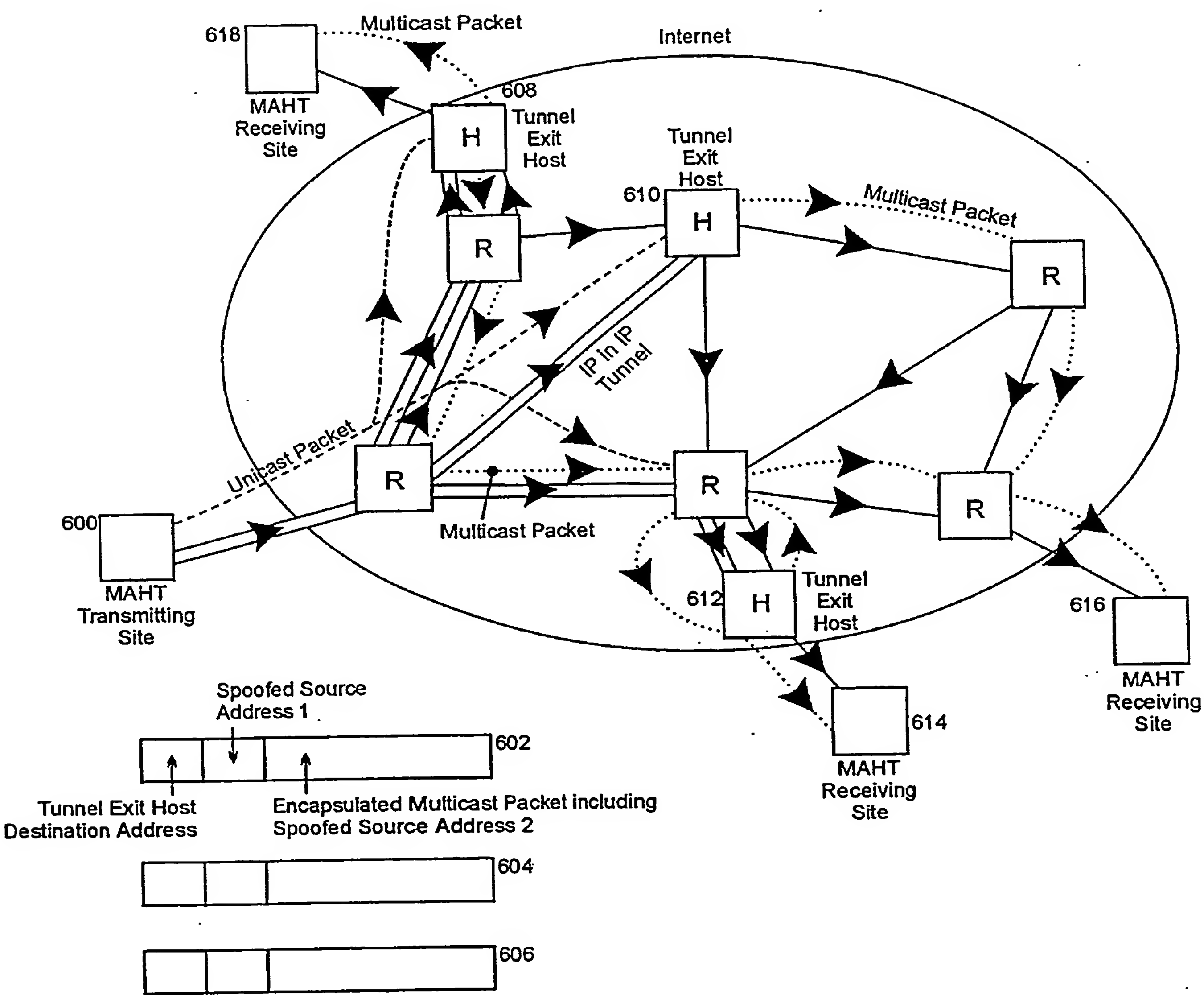

618
Multicast Packet
Internet
MAHT
Receiving
Site
608
H
Tunnel
Exit
Host
Tunnel
Exit
Host
610
H
Multicast Packet
R
R
IP in IP
Tunnel
Unicast Packet
R
R
R
R
600
MAHT
Transmitting
Site
Multicast Packet
612
H
Tunnel
Exit
Host
616
MAHT
Receiving
Site
614
MAHT
Receiving
Site
Spoofed Source
Address 1
602
Tunnel Exit Host
Destination Address
Encapsulated Multicast Packet including
Spoofed Source Address 2
604
606

Figure 7

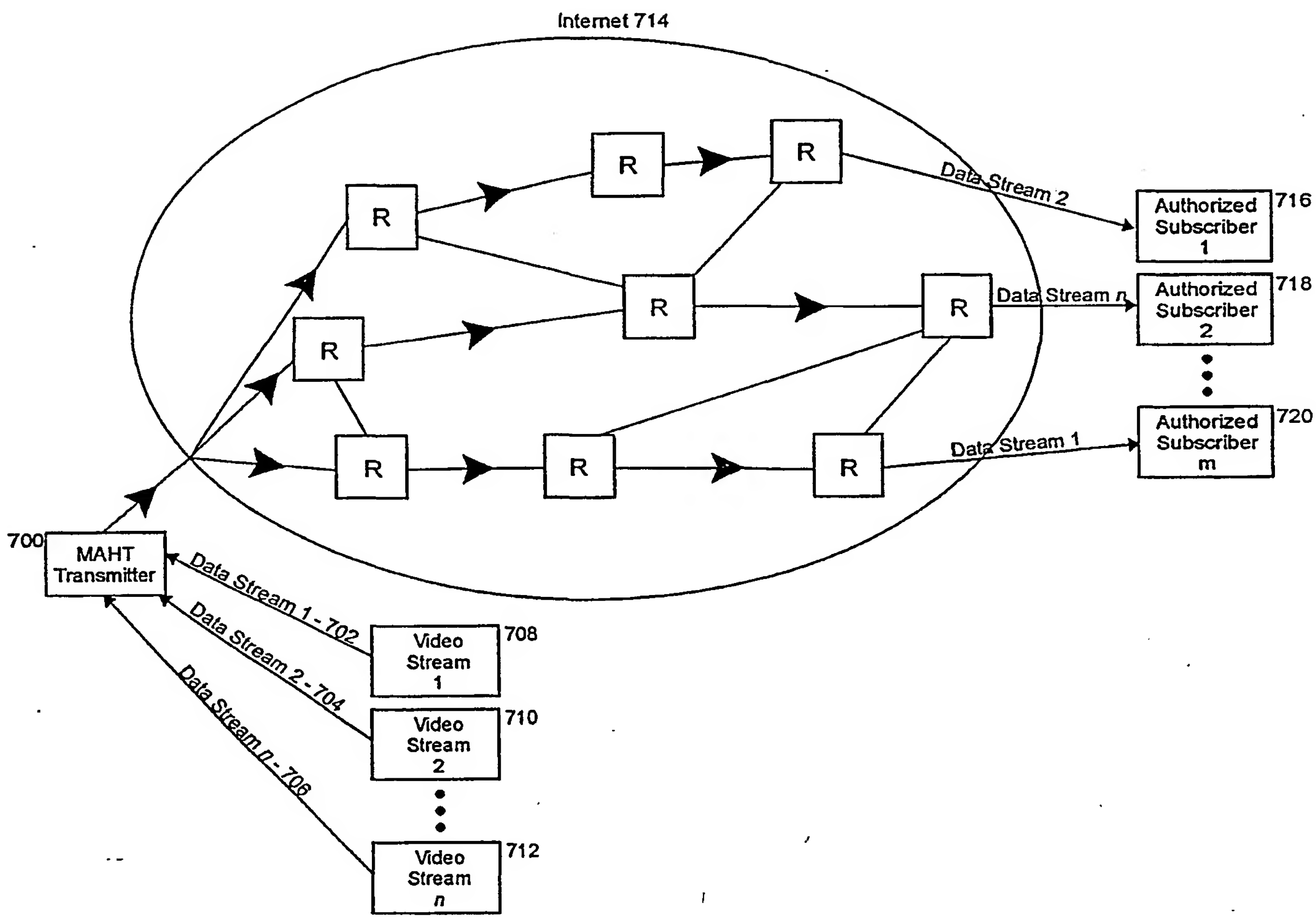

Internet 714
R
R
R
R
R
R
R
R
R
R
Data Stream 2
Data Stream n
Data Stream 1
Authorized Subscriber 1
716
Authorized Subscriber 2
718
Authorized Subscriber m
720
700
MAHT Transmitter
Data Stream 1 - 702
Data Stream 2 - 704
Data Stream n - 706
Video Stream 1
708
Video Stream 2
710
Video Stream n
712

Figure 8

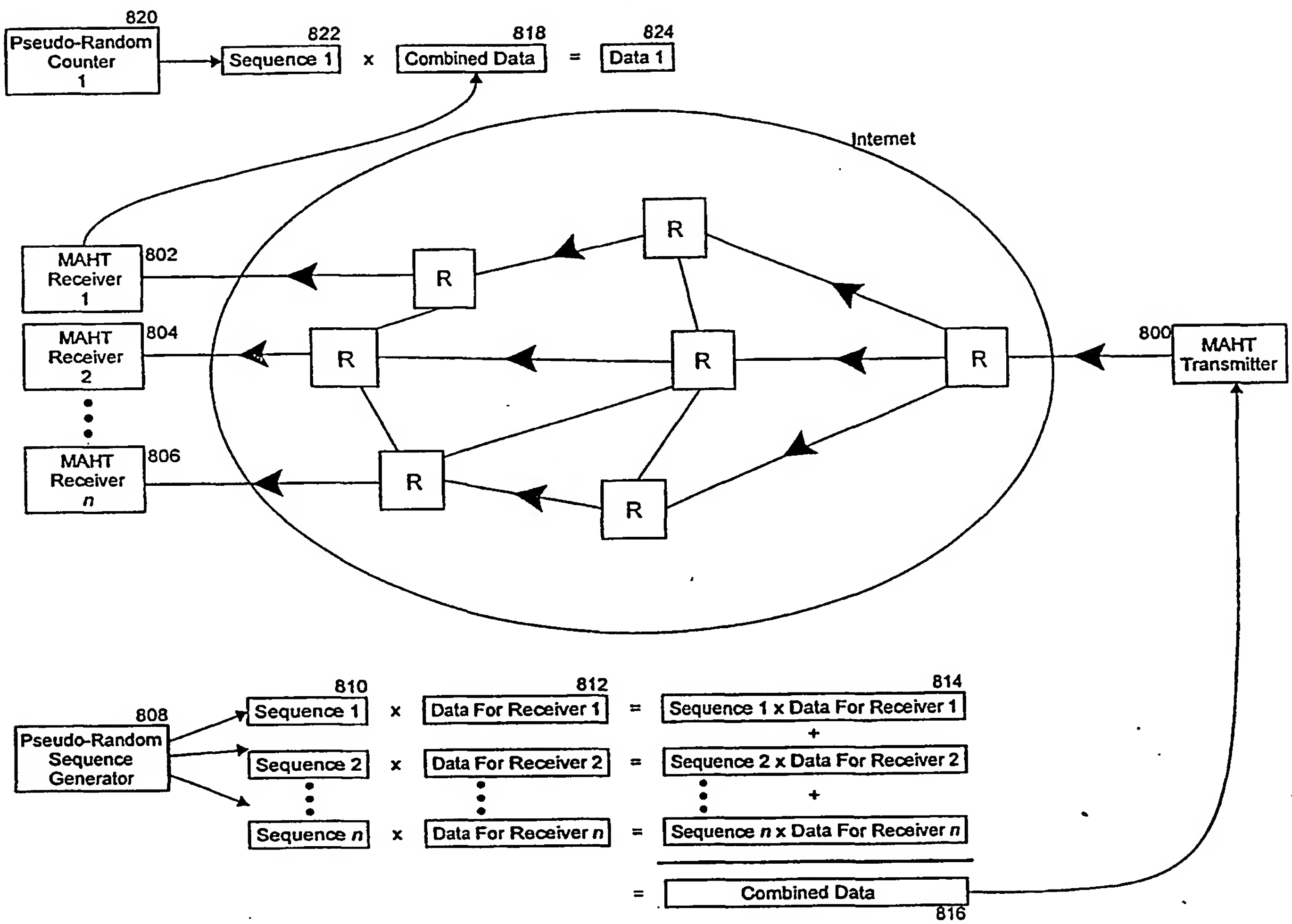
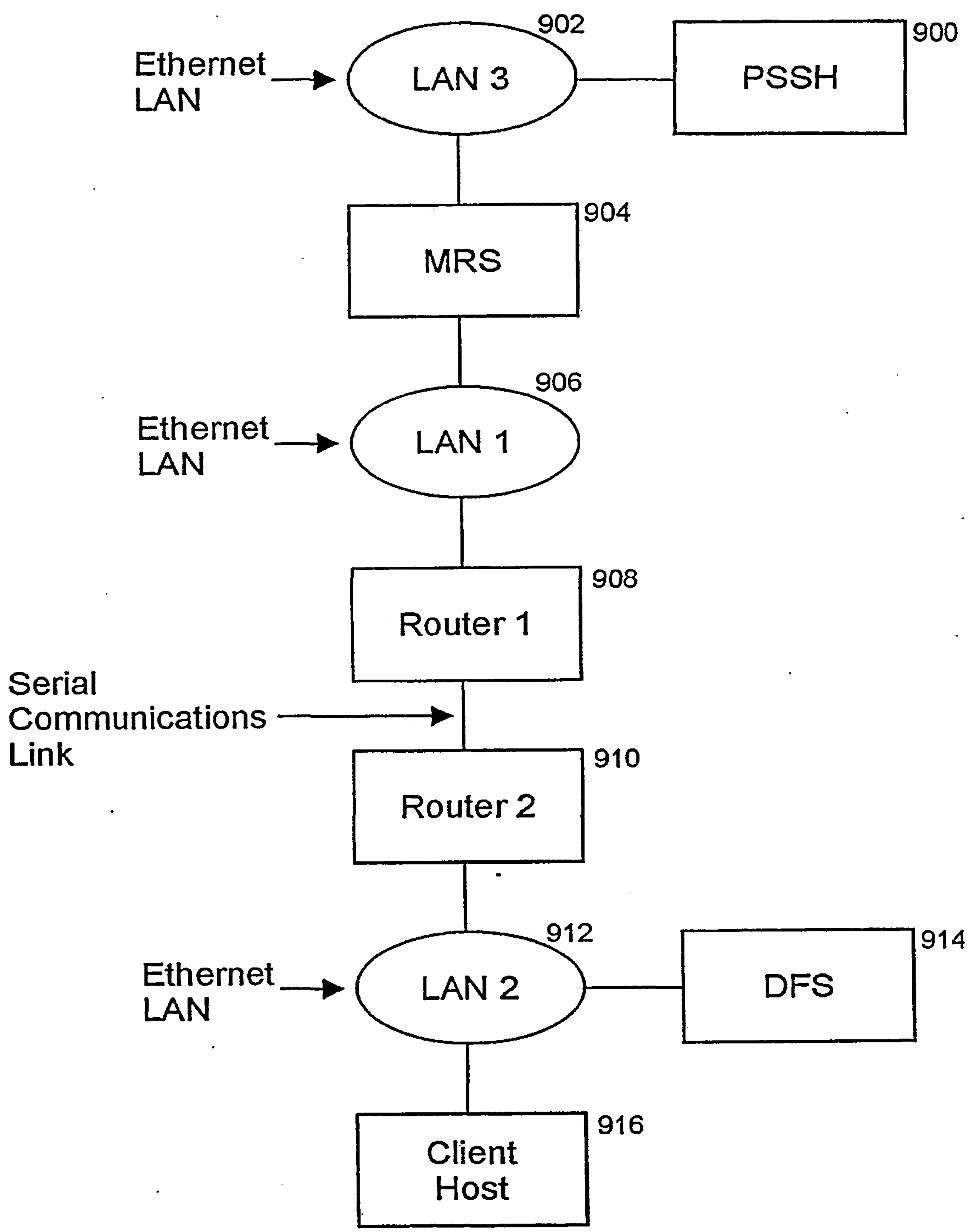

820
Pseudo-Random Counter 1
822
Sequence 1
x
818
Combined Data
=
824
Data 1
Internet
MAHT Receiver 1
802
MAHT Receiver 2
804
MAHT Receiver n
806
R
800
MAHT Transmitter
808
Pseudo-Random Sequence Generator
810
Sequence 1
Sequence 2
Sequence n
812
Data For Receiver 1
Data For Receiver 2
Data For Receiver n
814
Sequence 1 x Data For Receiver 1
Sequence 2 x Data For Receiver 2
Sequence n x Data For Receiver n
Combined Data
816

Figure 9


902
900
Ethernet LAN
LAN 3
PSSH
904
MRS
906
Ethernet LAN
LAN 1
908
Router 1
Serial Communications Link
910
Router 2
912
914
Ethernet LAN
LAN 2
DFS
916
Client Host

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
29 November 2001 (29.11.2001)

PCT

(10) International Publication Number
WO 01/091397 A3

(51) International Patent Classification[7]: H04L 12/18, 12/46

(21) International Application Number: PCT/CA01/00727

(22) International Filing Date: 22 May 2001 (22.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/575,544 22 May 2000 (22.05.2000) US

(71) Applicant: LADR IT CORPORATION [CA/CA]; 6 Sawgrass Circle, Ashton, Ontario K0A 1B0 (CA).

(72) Inventor: SHAWCROSS, Charles, Byron, Alexander; 6 Sawgrass Circle, Ashton, Ontario K0A 1B0 (CA).

(74) Agents: CASSAN, Lynn, S. et al.; Cassan MacLean, 401 - 80 Aberdeen Street, Ottawa, Ontario K1S 5R5 (CA).

(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

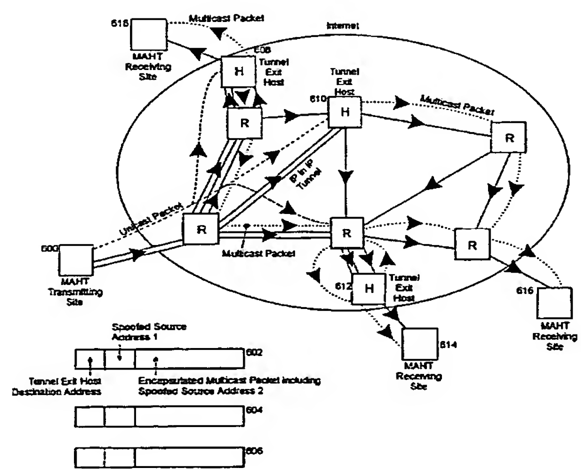
(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report: 8 August 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** METHOD AND SYSTEM FOR STOPPING HACKER ATTACKS



(57) **Abstract:** A method and system for Internet Protocol network communications and uses thereof for protecting Internet sites against denial of service and traffic analysis attacks on insecure public networks such as the Internet are provided. The method provides for communicating multicast packets between end stations, in a multicast IP network, on a chosen multicast IP address from a plurality of multicast IP addresses for multicast communication using a multicast address hopping technique. The technique selectively varies the chosen multicast IP address from the plurality of multicast IP addresses according to a predetermined scheme known to the end stations but not to unauthorized endstations. The packets are then communicated on the chosen multicast IP address. Indicia normally capable of identifying the source of the packets may be selectively varied to conceal the source of the packets. Further, use of the invention for Virtual Private Networks is also provided.

WO 01/091397 A3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/CA 01/00727

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/18 H04L12/46

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	GARBER L: "DENIAL-OF-SERVICE ATTACKS RIP THE INTERNET" COMPUTER, IEEE COMPUTER SOCIETY, LONG BEACH., CA, US, US, vol. 33, no. 4, April 2000 (2000-04), pages 12-17, XP000948670 ISSN: 0018-9162 the whole document ---	1-29
A	WO 99 48246 A (REUTERS AMERICA INCORPORATED) 23 September 1999 (1999-09-23) page 1, line 10 -page 2, last line -----	1-29

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 March 2002	20/03/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Ströbeck, A.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/CA 01/00727

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9948246 A	23-09-1999	AU 3092699 A	11-10-1999
		EP 1062766 A1	27-12-2000
		WO 9948246 A1	23-09-1999